BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 05. 2019 - 07. 05. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	Open Enterprise Server zraniteľnosť	Vysoká	**8.8**
03.	Rockwell Automation CompactLogix 5370 zraniteľnosti	Vysoká	**8.6**
04.	phpBB zraniteľnosť	Vysoká	**8.6**
05.	GE Communicator zraniteľnosť	Vysoká	**8.1**
06.	FileZilla bezpečnostná zraniteľnosť	Vysoká	**7.8**
07.	Check Point ZoneAlarm a Check Point Endpoint Security client zraniteľnosť	Vysoká	**7.8**
08.	Jenkins viacero zraniteľností zásuvných modulov	Vysoká	**7.7**
09.	Kubernetes kubectl zraniteľnosť	Vysoká	**7.7**
10.	Dell SupportAssist viacero zraniteľností	Vysoká	**7.6**
11.	Dovecot zraniteľnosti	Vysoká	**7.5**
12.	PrinterLogic Print Management Software zraniteľnosti	Vysoká	**7.5**
13.	Linux Kernel udp_gro_receive_segment zraniteľnosť	Vysoká	**7.5**
14.	IBM StoredIQ zraniteľnosť	Stredná	**6.1**
15.	F5 BIG-IP zraniteľnosti	Stredná	**6.0**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01380/2019/TS/OKB-130

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti v komponentoch IndexedDB a V8 umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.04.2019

CVE

CVE-2019-5824, CVE-2019-5825, CVE-2019-5826, CVE-2019-5827

Zasiahnuté systémy

Google Chrome verzie staršie ako 74.0.3729.131

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://chromereleases.googleblog.com/2019/04/stable-channel-update-for-desktop_30.html
https://www.tenable.com/plugins/nessus/124460
https://exchange.xforce.ibmcloud.com/vulnerabilities/160323
https://exchange.xforce.ibmcloud.com/vulnerabilities/160322
https://exchange.xforce.ibmcloud.com/vulnerabilities/160321

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Open Enterprise Server zraniteľnosť

Popis

Spoločnosť MicroFocus vydala bezpečnostné aktualizácie na svoje produkty Open Enterprise server 2015 a Open Enterprise server 2018.
Bližšie nešpecifikovanú zraniteľnosť v komponente NetStorage by vzdialený útočník mohol zneužiť na realizáciu XSS (Cross Site Scripting) útoku a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

02.05.2019

CVE

CVE-2019-3490

Zasiahnuté systémy

Open Enterprise Server 2015 Support Pack 1 verzie staršie ako Update 34 Security 4
Open Enterprise Server 2018 verzie staršie ako Update 7 Security 16
Open Enterprise Server 2018 Support Pack 1 verzie staršie ako Update 1 Security 18

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2019-3490
https://support.microfocus.com/kb/doc.php?id=7023828

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Rockwell Automation CompactLogix 5370 zraniteľnosti

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoje produkty CompactLogix 5370, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov SMTP paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

30.04.2019

CVE

CVE-2019-10952, CVE-2019-10954

Zasiahnuté systémy

Rockwell Automation CompactLogix 5370, Compact GuardLogix 5370 a Armor Compact GuardLogix 5370 verzie staršie ako 31.011

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-120-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

phpBB zraniteľnosť

Popis

Vývojári open source systému na tvorbu diskusných fór phpBB zverejnili aktualizáciu svojho produktu, ktorá rieši bezpečnostnú zraniteľnosť spôsobenú nedostatočnou implementáciou bezpečnostných opatrení. Zraniteľnosť v komponente Native Fulltext Search umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

29.04.2019

CVE

CVE-2019-9826

Zasiahnuté systémy

phpBB verzie staršie ako 3.2.6

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutého systému.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2019-9826
https://www.openwall.com/lists/oss-security/2019/04/29/3
https://www.phpbb.com/community/viewtopic.php?f=14&t=2509941

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GE Communicator zraniteľnosť

Popis

Spoločnosť GE vydala bezpečnostnú aktualizáciu na svoj produkt GE Communicator, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii dvoch zabudovaných používateľských účtov s predvolenými heslami a umožňuje vzdialenému, neautentifikovanému útočníkovi získať kontrolu nad systémom.

Dátum prvého zverejnenia varovania

02.05.2019

CVE

CVE-2019-6544, CVE-2019-6546, CVE-2019-6548, CVE-2019-6564, CVE-2019-6566

Zasiahnuté systémy

GE Communicator verzie staršie ako 4.0.517

Následky

Neoprávnený prístup do systému
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-122-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

FileZilla bezpečnostná zraniteľnosť

Popis

Vývojári FTP klienta FileZilla vydali aktualizáciu na svoj produkt ktorá, opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

29.05.2019

CVE

CVE-2019-5429

Zasiahnuté systémy

FileZilla verzie staršie ako 3.41.0-rc1

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/160288
https://www.tenable.com/security/research/tra-2019-14

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Check Point ZoneAlarm a Check Point Endpoint Security client zraniteľnosť

Popis

Spoločnosť Check Point vydala bezpečnostné aktualizácie na svoje produkty Check Point ZoneAlarm a Endpoint Security client, ktoré obsahujú bezpečnostnú zraniteľnosť spôsobenú nedostatočnou implementáciou bezpečnostných mechanizmov. Zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

22.04.2019

CVE

CVE-2019-8452

Zasiahnuté systémy

Check Point Endpoint Security client starší ako e80.96
Check Point ZoneAlarm starší ako 15.4.062

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2019-8452?cpeVersion=2.2#vulnConfigurationsArea

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Jenkins viacero zraniteľností zásuvných modulov

Popis

Vývojári automatizačného servera Jenkins vydali aktualizácie na zásuvné moduly, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia z týchto zraniteľností sa nachádza v SiteMonitor zásuvnom module a spôsobuje deaktiváciu SSL/TLS validácie certifikátov pre celú Jenkins JVM, čo môže byť zneužité na vykonanie ďalších útokov.

Dátum prvého zverejnenia varovania

30.04.2019

CVE

CVE-2019-10300, CVE-2019-10307, CVE-2019-10308, CVE-2019-10309, CVE-2019-10310, CVE-2019-10311, CVE-2019-10312, CVE-2019-10313, CVE-2019-10314, CVE-2019-10315, CVE-2019-10316, CVE-2019-10317, CVE-2019-10318

Zasiahnuté systémy

SiteMonitor Plugin verzie staršie ako 0.6
Ansible Tower Plugin verzie staršie ako 0.9.2
Aqua MicroScanner Plugin verzie staršie ako 1.0.6
Azure AD Plugin verzie staršie ako 0.3.4
GitHub Authentication Plugin verzie staršie ako 0.32
SiteMonitor Plugin verzie staršie ako 0.6
Static Analysis Utilities Plugin verzie staršie ako 1.96
Jenkins GitLab Plugin 1.5.11

Následky

Neoprávnená zmena v systéme
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://jenkins.io/security/advisory/2019-04-30/
https://exchange.xforce.ibmcloud.com/vulnerabilities/160308
https://exchange.xforce.ibmcloud.com/vulnerabilities/160309
https://exchange.xforce.ibmcloud.com/vulnerabilities/160310
https://exchange.xforce.ibmcloud.com/vulnerabilities/160311
https://exchange.xforce.ibmcloud.com/vulnerabilities/160312
https://exchange.xforce.ibmcloud.com/vulnerabilities/160313
https://exchange.xforce.ibmcloud.com/vulnerabilities/160314
https://exchange.xforce.ibmcloud.com/vulnerabilities/160315
https://exchange.xforce.ibmcloud.com/vulnerabilities/160316
https://exchange.xforce.ibmcloud.com/vulnerabilities/160317
https://exchange.xforce.ibmcloud.com/vulnerabilities/160318
https://exchange.xforce.ibmcloud.com/vulnerabilities/160319
https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0783
https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0786
https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0788

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Kubernetes kubectl zraniteľnosť

Popis

Vývojári orchestrátora kontajnerov Kubernetes vydali bezpečnostnú aktualizáciu svojho produktu, ktorá upravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov pri spracovaní .tar súborov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

04.04.2019

CVE

CVE-2019-1002101

Zasiahnuté systémy

Kubernetes verzie 1.14 (.0) a staršie

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59908
https://github.com/kubernetes/kubernetes/pull/75037

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell SupportAssist viacero zraniteľností

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt Dell SupportAssist predinštalovaný v notebookoch Dell, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente, prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.04.2019

CVE

CVE-2019-3718, CVE-2019-3719

Zasiahnuté systémy

Dell SupportAssist Client verzie staršie ako 3.2.0.90

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.dell.com/support/article/sk/sk/skdhs1/sln316857/dsa-2019-051-dell-supportassist-client-multiple-vulnerabilities?lang=en
https://thehackernews.com/2019/05/dell-computer-hacking.html
https://www.zdnet.com/article/dell-laptops-and-computers-vulnerable-to-remote-hijacks/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dovecot zraniteľnosti

Popis

Vývojári emailového servera Dovecot vydali bezpečnostnú aktualizáciu, ktorá opravuje dve zraniteľnosti. Bezpečnostné zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravenej správy spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.04.2019

CVE

CVE-2019-11494, CVE-2019-11499

Zasiahnuté systémy

Dovecot verzie staršie ako 2.3.6

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/160443
https://exchange.xforce.ibmcloud.com/vulnerabilities/160444
https://seclists.org/oss-sec/2019/q2/82

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PrinterLogic Print Management Software zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o viacerých bezpečnostných zraniteľnostiach v produkte PrinterLogic Print Management Software. Najzávažnejšia zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

03.05.2019

CVE

CVE-2018-5408, CVE-2018-5409, CVE-2019-9505

Zasiahnuté systémy

PrinterLogic Print Management Software verzia 18.3.1.96 a staršie

Následky

Vykonanie škodlivého kódu
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Tiež odporúčame aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/160528
https://exchange.xforce.ibmcloud.com/vulnerabilities/160527
https://exchange.xforce.ibmcloud.com/vulnerabilities/160526
https://www.kb.cert.org/vuls/id/169249/
https://threatpost.com/printerlogic-remote-code-execution/144383/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux Kernel udp_gro_receive_segment zraniteľnosť

Popis

Vývojári Linux Kernel zverejnili bezpečnostnú zraniteľnosť, ktorá spočíva v nedostatočnej implementácii bezpečnostných mechanizmov. Zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených UDP paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.05.2019

CVE

CVE-2019-11683

Zasiahnuté systémy

Linux Kernel 5.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/160517
https://seclists.org/oss-sec/2019/q2/86
https://git.kernel.org/pub/scm/linux/kernel/git/davem/net.git/commit/?id=4dd2b82d5adfbe0b1587ccad7a8f76d826120f37

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM StoredIQ zraniteľnosť

Popis

Spoločnosť IBM informovala o bezpečnostnej zraniteľnosti v produkte IBM StoredIQ. Zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravenej webovej stránky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

30.04.2019

CVE

CVE-2019-4166

Zasiahnuté systémy

Všetky verzie IBM StoredIQ od 7.6.0.0 (vrátane) do 7.6.0.18 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame zabezpečiť systém podľa návodu zverejnenom na https://www-01.ibm.com/support/docview.wss?uid=ibm10881404
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2019-4166?cpeVersion=2.2#vulnConfigurationsArea
https://www-01.ibm.com/support/docview.wss?uid=ibm10881404

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.0
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

F5 BIG-IP zraniteľnosti

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoj produkt BIG-IP, ktorá opravuje šesť bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

30.04.2019

CVE

CVE-2019-6614, CVE-2019-6615, CVE-2019-6616, CVE-2019-6617, CVE-2019-6618, CVE-2019-6619

Zasiahnuté systémy

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator, WebSafe) verzie staršie ako 14.1.0.2, 13.1.1.5, 12.1.4.1, 11.6.4, 11.5.9

Následky

Eskalácia privilégií
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K46524395
https://support.f5.com/csp/article/K82814400
https://support.f5.com/csp/article/K07702240
https://support.f5.com/csp/article/K38941195
https://support.f5.com/csp/article/K87659521
https://support.f5.com/csp/article/K94563344

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01380/2019/TS/OKB-130